UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,903	01/10/2001	Luis M. Ortiz	K1033	8298

7590 03/06/2007

ORTIZ & LOPEZ, PLLC
Patent Attorney
P. O.4484
Albuquerque,, NM 87196-4484

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.**	**Applicant(s)**	
	09/757,903	ORTIZ, LUIS M.	
	Examiner	**Art Unit**	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-23,25-34 and 36-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12, 14-23, 25-34, and 36-44* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on December 7, 2006. Claims 1-12, 14-23, 25-34, and 36-44 are currently being considered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-12, 14-23, 25-34, and 36-44 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claim 44 is objected to because of the following informalities: The claim in third limitation states that there are "two" biometric attributes, which are randomly selected for comparison to the "one" biometric input. Then in the final limitation of the claim, a user is permitted to perform the activity if "one" biometric attribute is matched. This creates confusion about the number of biometric inputs and attributes which are requested and compared. For the purposes of examination, it is interpreted that "two" biometric attributes are input and compared. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 4 recites the limitation “said server” in the first line of the second limitation. Claim 1 was amended to cancel the limitations with a server contained in the language, and therefore, there is now antecedent basis for “said server” in the claims. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-6, 8-12, 14, 16, 17-21, 23, 25-28, 30-34, 36, and 38-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Lewis (U.S. Patent 6,313,391).

Regarding claim 1, Lewis discloses:

A method for biometrically securing access to an electronic system, said method comprising the steps of:

obtaining identification of a user from a smart card presented to the electronic system by said user (column 3 lines 47-65, column 7 lines 36-65), *wherein a biometric input is received by the smart card and used in verifying the identity of an individual*;

prompting said user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from said user profile containing biometric attributes of said user (column 5 lines 1-9, column 7 lines 36-65), *wherein the system may require the user to speak one of any specific code words previously recorded by the user*;

permitting said user to perform a user-desired activity with the electronic system if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches said at least one biometric attribute randomly selected from said user profile (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account.*

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said computer network is a secure computer network (column 5 lines 64-67, column 9 lines 31-38), *wherein the network can support an ATM transaction.*

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user profile is stored in a biometric broker (column 10 lines 8-23), *wherein the biometric information may be retrieved from a central database.*

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 further comprising the steps of:

obtaining at least one biometric attribute from said user from compilation in said user profile (column 4 lines 40-57), *wherein at the time an account is opened, the user provides biometric input to be stored on the smart card and/or the database*;

compiling said user profile (column 4 lines 40-57), *wherein the biometric input is transformed into digital format and stored*; and

storing said user profile in said server accessible by at least one biometric user interface associated with said electronic system (column 4 lines 40-57), *wherein at the time an account is opened, the user provides biometric input to be stored on the smart card and/or the database*.

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Lewis discloses:

The method of claim 4 further comprising the steps of:

permitting the user to modify said user profile, in response to approval of a request by said user *(column 5 lines 31-59), wherein the user can change a PIN in a bank system (column 1 lines 56-57) at any time.*

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 further comprising the step of:

comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account.*

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises at least one wireless device that operates with a wireless network (column 9 lines 38-46).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises at least one computer workstation operable over an associated network (column 3 lines 47-65).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises an automated teller machine (column 3 lines 47-52).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises a secured entry system to a secured environment (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises a wireless network (column 9 lines 38-46).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises a wireless device (column 9 lines 38-46).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises a financial transaction (column 3 lines 47-52).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises an ATM transaction (column 3 lines 47-52).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises access to a secure area (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 19 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises access to data from said electronic system (column 3 lines 47-52).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises execution of a mechanical activity (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 further comprising the step of:

initiating access to said electronic system utilizing only one biometric input to said electronic system (column 8 lines 7-15).

Regarding claim 23, Lewis discloses:

A system for biometrically securing access to an electronic system, said system comprising:

an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from a user profile accessible by the electronic system from a smart card presented to the electronic system by the user (column 5 lines 1-9, column 7 lines 36-65), wherein said smart card is adapted to store at least one user profile including biometric attributes and provide said electronic system access to at least one user profile (column 3 lines 47-65, column 7 lines 36-65), *wherein a biometric input is received by the smart card and used in verifying the identity of an individual*;

a smart card reader associated with said electronic system (column 4 lines 27-64); and

a biometric user interface associated with said electronic system adapted to enable said user to input at least one biometric to said electronic system for comparison to at least one biometric attribute randomly selected by said electronic system from said user profile (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account;*

wherein said electronic system is adapted to permit said user to perform a user-desired activity, if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile by said electronic system (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account.*

Claim 25 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user profile is accessible from a biometric broker via a secure network connection (column 10 lines 8-23), *wherein the biometric information may be retrieved from a central database.*

Claim 26 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein:

at least one biometric attribute is obtained from said user for compilation in said user profile (column 4 lines 40-57), *wherein at the time an account is opened, the user provides biometric input to be stored on the smart card and/or the database.*

Claim 27 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user is permitted to modify said user profile, in response to approval of a request by said user *(column 5 lines 31-59), wherein the user can change a PIN in a bank system (column 1 lines 56-57) at any time.*

Claim 28 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 further comprising:

module for comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account.*

Claim 30 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises at least one wireless device that operates with a wireless network (column 9 lines 38-46).

Claim 31 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises at least one computer workstation accessible over said computer network (column 3 lines 47-65).

Claim 32 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises an automated teller machine (column 3 lines 47-52).

Claim 33 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises a secured entry system to a secured environment (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate*.

Claim 34 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said computer network comprises a wireless network (column 9 lines 38-46).

Claim 36 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises a wireless device (column 9 lines 38-46).

Claim 38 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises a financial transaction (column 3 lines 47-52).

Claim 39 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises an ATM transaction (column 3 lines 47-52).

Claim 40 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises access to a secure area (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 41 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises access to data from said electronic system (column 3 lines 47-52).

Claim 42 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises execution of a mechanical activity (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 43 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein access to said electronic system is initiated utilizing only one biometric attribute input to said electronic system (column 8 lines 7-15).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 7, 15, 29, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 6,213,391) in view of Price-Francis (U.S. Patent 5,815,252).

Claim 7 is rejected as applied above in rejecting claim 6. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 15 is rejected as applied above in rejecting claim 6. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 29 is rejected as applied above in rejecting claim 28. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 37 is rejected as applied above in rejecting claim 23. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

7. Claims 22, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 6,213,391) in view of Abrahams (U.S. Patent 6,944,773).

Regarding claim 22, Lewis discloses:

A method for biometrically securing access to an electronic system, said method comprising the steps of:

obtaining identification of a user from a smart card presented to the electronic system by said user (column 3 lines 47-65, column 7 lines 36-65), *wherein a biometric input is received by the smart card and used in verifying the identity of an individual*;

based on said identification, using a computer network to obtain a user profile associated with said user from a remote server, said user profile including biometric attributes (column 4 lines 55-57, column 10 lines 10-22), *wherein the profile can be fetched from a central database.*

Lewis does not explicitly mention prompting a user for two biometric attributes and if these biometric attributes are successful, allowing the user to perform a user-desired activity. Abrahams discloses prompting a user for two or more biometric attributes (fingerprints) and if the fingerprints match, authenticating the user to perform a task (column 3 lines 27-50). Abrahams and Lewis are analogous arts in that both use biometric attributes to authenticate a user to perform a task including financial transactions. Allowing the system of Lewis to check for multiple biometrics would be feasible as the smart card and the biometric database of Lewis store multiple biometric attributes of each user (column 5 lines 1-9). It would have been obvious to one of ordinary skill in the art at the time of invention to prompt the user for two biometric attributes before authenticating the user so that the likelihood of fraud is reduced (Abrahams: column 4 lines 15-22, column 4 lines 57-59).

Regarding claim 44, Lewis discloses:

A system for biometrically securing access to an electronic system, said system comprising:

an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile accessible by the electronic system over a computer network from a remote server, said electronic system including access to a remote server through electronic connection to a computer network and said remote server adapted to store at least one user profile including biometric attributes and provide said electronic system to said at least one user profile (column 4 lines 55-57, column 10 lines 10-22), *wherein the profile can be fetched from a central database.*;

a smart card reader associated with said electronic system (column 4 lines 27-64).

Lewis does not explicitly mention prompting a user for two biometric attributes and if these biometric attributes are successful, allowing the user to perform a user-desired activity. Abrahams discloses prompting a user for two or more biometric attributes (fingerprints) and if the fingerprints match, authenticating the user to perform a task (column 3 lines 27-50). Abrahams and Lewis are analogous arts in that both use biometric attributes to authenticate a user to perform a task including financial transactions. Allowing the system of Lewis to check for multiple biometrics would be feasible as the smart card and the biometric database of Lewis store multiple biometric attributes of each user (column 5 lines 1-9). It would have been obvious to one of ordinary skill in the art at the time of invention to prompt the user for two biometric attributes before authenticating the user so that the likelihood of fraud is reduced (Abrahams: column 4 lines 15-22, column 4 lines 57-59).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
03/01/2007

SYED ZIA 03/01/2007
PRIMARY EXAMINER
AU 2131